House Committee on Homeland Security
Subcommittee on Economic Security, Infrastructure Protection and Cyber Security

Hearing on "SCADA and the Terrorist Threat: Protecting the National's Critical Control Systems"

311 Cannon House Office Building
October 18, 2005

Testimony of Dr. K. P. Ananth
Associate Laboratory Director, National & Homeland Security
Idaho National Laboratory
Idaho Falls, Idaho

Chairman Lungren and distinguished members of the Homeland Security Subcommittee:

I am Dr. K. P. Ananth, Associate Laboratory Director for National and Homeland Security at the Idaho National Laboratory (INL), a DOE national laboratory. It is a privilege and honor for me to appear before you to represent the work being carried out at INL in support of our national efforts, undertaken in both the federal and private sectors, to protect U.S. critical infrastructure. In this testimony, I will give you a brief background on INL and its mission, and a summary of our unique capabilities as they relate to Supervisory Control and Data Acquisition (SCADA), Critical Infrastructure Protection (CIP) and Cyber Security. I will also discuss key federal and commercial programs carried out at the Laboratory to support industry and end users, and identify the challenges we face along with some recommendations.

INL and its Mission

The Idaho National Laboratory had its origin as the National Reactor Testing Station in 1949 in Idaho Falls with a mission to design, engineer, develop a prototype, and test an electricity producing nuclear reactor. Within two (2) years, in December 1951, INL successfully demonstrated the first electric power reactor and, soon thereafter, developed the first prototype nuclear reactor for the nuclear submarine Nautilus. For more than 50 years, the laboratory has been a critical asset within the National Laboratory system as an engineering, prototyping and testing resource, with 52 reactors built and operated on the 890 square mile reservation in southeastern Idaho. Beginning in the 1950s, the Laboratory began to support major Department of Defense programs, including training of thousands of Navy nuclear operators; earlier the Laboratory was involved in the development and testing of naval guns and ordnance. In 1985, the Laboratory was selected to produce armor for the Army's Abrams tank using depleted uranium, and earlier this year we successfully completed our twentieth anniversary on the program.

To support these varied missions, INL has developed a significant infrastructure on the Idaho desert. INL carries the distinction of a vast, remote, and secure heavily-invested site complex with "one-of-a-kind" test beds and facilities for nuclear research and development (R&D), explosives detection and testing, unmanned aerial and ground vehicles payload testing, physical security, cyber security and critical infrastructure protection.

Mindful of the rich assets at INL, the Department of Energy issued a Request for Proposal (RFP) in 2004 to manage and operate INL with the mission of ensuring the nation's energy security with safe, competitive, and sustainable energy systems and providing unique national and homeland security capabilities. Two areas were specifically called out within national and homeland security for the Laboratory: nuclear nonproliferation and critical infrastructure protection. On February 1, 2005, the new contract to operate the Laboratory was implemented, making the critical infrastructure protection mission of the Idaho National Laboratory unique within the National Laboratory system. We are hard at work fulfilling this mandate.

Today I will focus on how we are leveraging our efforts with DHS and DOE in the area of improving control systems security across all critical infrastructure sectors by reducing cyber security vulnerabilities and risk.

INL's Unique Assets

With more than five decades of experience in establishing, developing and maintaining critical infrastructure systems, INL has created several recognized and integrated capabilities to provide real solutions to our customers in critical infrastructure protection and cyber security. INL has focused in three major areas – process control systems, cyber security, and wireless technology.

Process Control Systems (PCS) and SCADA – Our location and operational infrastructure provides the ultimate proving ground for analysis and assessment of real-world critical infrastructure components. INL has become the logical home for significant portions of the National SCADA Test Bed and has become the focal point for research and testing of control systems and cyber security with a direct benefit of increasing the security of these systems. INL operates a power distribution control center, a pilot chemical plant, and 61 miles of 138 kV transmission line with seven substations and a dedicated control room on our 890 square mile site. It is the combination of this infrastructure, a program with current access to commercial control systems from principal global vendors (e.g., ABB, AREVA, GE, METSCO, Micro Motion, [Emerson], Rockwell Automation, Siemens), and our research expertise and partners that enables us to conduct offline and full-scale testing in a real life environment. This unique capability is helping to research and develop solutions that will strengthen our nation's industrial control systems and physical components of our infrastructures from attacks by viruses, hackers, and terrorists.

Cyber Security – the INL Cyber Security Group's intimate familiarity with various hacker methodologies enables us to generate exploits and assessment tools for use in testing the security of Critical Infrastructure control system environments. Focused on multi-tier attack vectors and full spectrum threat actors, the team provides a credible representation of cyber threats and then conducts cutting edge research into advanced mitigation strategies and solutions. Coupled with our academic and industry partners in this area, we are striving to effectively address current challenges while advancing the state-of-the-art in detecting hacker signatures. We have invested resources to explore the cyber security vulnerabilities of Portable Electronic Devices (PEDs) technology. INL is pursuing commercial and government partnerships to address vulnerabilities in PEDs technology because these devices are becoming more prolific and have crept into new control systems.

Wireless Technology – INL's Wireless Test Bed and telecommunications infrastructure provides access to advanced, next generation communication technology and current communication systems to analyze vulnerabilities, analyze new protocols and operational performance, and develop risk mitigating solutions. INL's location providing a low RF background, our National Telecommunications and Administration (NTIA) experimental radio station status, full-scale isolated communications networks, and ability to connect to functional systems has attracted industry (e.g., Bechtel Telecommunications, Nokia, AT&T Wireless) and government customers. Bechtel Telecom, through a Cooperative Research and Development Agreement (CRADA), has made a significant investment at the Laboratory in this area. These attributes afford us the unique opportunity to holistically analyze both performance and risk of entire systems, develop wireless security solutions for our nation's complex, interconnected infrastructures, and improve robustness of communication links for emergency responders.

The importance of these core assets can not be overlooked, representing a national resource that provides access to control system hardware and applications, functioning transmission and distribution assets, wireless local and metro area networks, advanced radio, microwave, fiber optic and satellite communications, mesh networks and personal electronic devices (PEDs). Additional assets include unmanned aerial vehicles (UAVs), explosives detection, testing and blast mitigation systems. Perhaps more importantly, our current network of industry participants and top shelf researchers across the nation enable INL to address the most challenging issues in CIP.

These are the elements – housed in our comprehensive test range, designed to be full-scale in nature, representative of real world infrastructures and capable of being isolated – that uniquely position the federal government, national laboratories, and industry to be successful in identifying and managing risk to our nation's critical infrastructure. To the best of our knowledge, there is no similar facility in the world. And, the cache of over 100 experienced scientists, engineers, and technicians working in INL's SCADA/Cyber Security groups are aware of the great responsibility that comes with managing these resources and the significance of our mission to assist in securing the control systems of our nation's critical infrastructure.

With this knowledge, we have focused on developing extensive collaborations on our programs and continually strive to bring the best-in-class institutions to help in developing solutions to this complex challenge. Our collaborators in this area include other national laboratories, National Institute of Standards and Technology (NIST), American Society of Mechanical Engineers (ASME), Instrumentation Systems and Automation Society (ISA), Carnegie Mellon University (CMU), Dartmouth University (DU), University of Idaho (UoI), British Columbia Institute of Technology (BCIT), and others such as North American Electric Reliability Council (NERC), Electric Power Research Institute (EPRI), Chemical Industry Data Exchange (CIDX), Decision Analytics Corporation (DAC), KEMA Consulting and Bearing Point.

Key Programs Conducted at INL and Results Achieved

Our two primary programs in Cyber Security and Critical Infrastructure Protection are with the Department of Homeland Security National Cyber Security Division and Department of Energy Office of Electricity Delivery and Energy Reliability. INL is supporting both programs with a team of talented people from other national labs, academia and industry based on their best-in-class core competencies and the needs of the program.

The DHS program is known as the "US-CERT Control Systems Security Center (CSSC) Program." This program is aimed at improving control systems security across all critical infrastructure sectors by reducing cyber security vulnerabilities and risk. One of the key tasks of this program was the design of a cyber security protection framework consisting of a comprehensive set of requirements, graded recommendations/solutions, and automated self-assessment tools for all sectors to use to enhance the security of their control systems (e.g., SCADA, DCS) against cyber attack. The draft framework was issued in July 2005 and reviewed with 20 industry control systems and cyber experts; and a second review occurred in August with several key industry security managers. Comments to date have been:

"….framework provides a centralized, organized approach to Control System security…"
"….provides actionable recommendations…"
"….provides a benchmark and metrics for cyber security protection..."
"….will help consolidate the efforts by the Standard bodies…"
"…provides for cross platform standardization across vendor products…"
"...impressed with the automated self-assessment tools that will measure improvement
over time…"

We have plans to work with NIST and ISA over the next three months to assist us in implementing the cyber security framework for self assessment. We will also work with facilities in several key sectors in FY-06 to pilot and validate the framework. A key component of the self assessment will be a risk reduction tool that helps companies prioritize vulnerabilities that are found when assessing requirements and potential consequences.

Additionally, the program also developed a quick response cell to support US CERT in handling control system specific incidents/events. We have assisted in preparing cyber security bulletins and providing Tier II support for reported events to the US-CERT.

Over the last two years, we have collaborated with DHS and DOE to significantly increase the capabilities of our extensive cyber test bed. This capability includes ten (10) SCADA test beds and three (3) fully functioning systems that are ready and are currently testing vendor systems and specific tools to reduce cyber vulnerabilities. On the CSSC program, we are currently testing three (3) vendor control systems and have already identified significant vulnerabilities on the first two systems. The vendors are evaluating the results and our recommendations.

The purpose of this program is to reduce risk to key infrastructure from cyber attack by enhancing the security of control systems. To that end, we have developed a risk assessment methodology for control systems to measure vulnerability reduction and we have developed decision analysis tools. We have started validating these tools by analyzing test results and attack scenarios.

Our industry outreach efforts provide unique training by demonstrating how an attack may propagate through the business system to critical control systems with an emphasis on how to mitigate the effects of such an attack. These awareness demonstrations and training activities are ongoing with positive feedback from industry and government participants. The tabletop demonstrations have included live demonstrations of attacks/effects on small scale representative control systems for chemical and electric system processes and demonstrations of attack mitigation strategies. We have held these demonstrations at nine (9) venues across the U.S. with over 460 end users participating from a wide variety of industries to include control systems/cyber security organizations and federal, state and local government agencies.

Through this program, we are also providing SCADA and process control security training for the protection of dams and hydroelectric facilities to system users in the Department of Interior's Bureau of Reclamation.

The DOE program, known as the "National SCADA Test Bed (NSTB) performs testing and analysis of SCADA systems representative of those used throughout the energy sector to identify, validate and reduce cyber vulnerabilities. The second objective is to identify best practices for design and deployment of secure control systems and to support institutionalization of those best practices in government and industry standards. The NSTB is a joint effort between Sandia National Laboratory and Idaho National Laboratory. The NSTB effort is managed by the INL and includes, Pacific Northwest National Laboratory (PNNL), Argonne National Laboratory (ANL), and the SCADA vendor community (ABB Network Management, AREVA T&D Automation, GE Energy Management Systems, Siemens Power Transmission and Distribution), as well as computer system vendors such as IBM, HP, and Sun Systems. Key accomplishments on this program include:

- The NSTB has identified SCADA vulnerabilities in the four systems INL has tested, worked with the SCADA vendors to define/develop fixes where needed, and verified the fixes through follow-on testing. SCADA vendors have improved new releases and developed patches to mitigate significant security weakness. These risk reducing actions will directly benefit many of the nation's critical infrastructure organizations.
- We have shared the findings from these SCADA system vulnerability assessments, in various levels of detail, with over 230 representatives from 100 major industry owner/user organizations through invited presentations at SCADA vendor users' group meetings.
- We have issued detailed test reports of the SCADA assessments to the respective vendors. One of the vendors is sharing their assessment report, under tight non-disclosure agreements, with all interested users.
- Through the participation of SCADA vendors who have been willing to loan their systems to INL on the NSTB program for an extended time, we have established an extensive, representative environment for searching out typical security vulnerabilities and for testing solutions.

We developed and presented a NERC-certified training course on SCADA security. Based on feedback from the initial presentation of various courses (NERC and others) to over 350 participants, we are expanding the content and are now responding to requests for additional presentations.

Commercial Programs – INL has helped industry develop and deploy more secure digital control/SCADA systems, through vulnerability discovery, validation and mitigation, standards development and secure software technology.

Specifically, the INL managed National SCADA Test Bed Program (NSTB) has worked with global control system software vendors to promote more secure , innovative installation and implementation of their products, where such efforts are consistent with recognized industry guidelines and best practices. The program has discovered existing weaknesses in deployed systems as well as design weaknesses in future control systems. The program has evaluated technology from providers representing 80% of the electrical grid control system market, working closely with engineering teams of four (4) global providers.

We have worked with control system owners and operators across multiple sectors to evaluate and enhance security of existing technology deployments. These companies took advantage of the unique knowledge-base and trusted relationships at the Lab as an important element to their overall approach to critical systems risk management. Companies have also turned to us when things go wrong with the systems to assist in evaluating particular events to determine if directed or non-directed attacks might have occurred.

With most of the critical infrastructure residing in the private sector we felt it was appropriate to submit just a few comments from the asset owners themselves. These perspectives come from private sector organizations from the trenches to the executive offices best demonstrating the value of government sponsored CIP initiatives at INL:

1. David Norton, Transmission IT Security program manager for Entergy – New Orleans (the second largest generator of electricity in the U.S. delivering electricity to 2.7 million customers), wrote "We are in dire need of INL, its mission, and its uniquely qualified staff. I know of no other entity in North America doing anything like what they are doing in the field of SCADA control system security, and certainly not to the level of excellence that I and my peers in the industry have witnessed."
2. Cheryl Santor, Information Security Manager, Metropolitan Water in California (one of the largest water systems servicing 5,200 square miles in Los Angeles, Orange, San Diego, Riverside, San Bernardino and Ventura Counties with 18 million customers), wrote "The INL provides a knowledge base from which all organizations using SCADA and Process Controls can benefit….in order to secure their critical resources."
3. Phil Harris, CEO of PJM (Ensuring the reliability of the largest centrally dispatched Control area in North America by coordinating the movement of electricity in all parts of Delaware, Illinois, Indiana, Kentucky, Maryland, Michigan, New Jersey, North Carolina, Ohio, Pennsylvania, Tennessee, Virginia, West Virginia, and the District of Columbia), wrote "PJM feels it is important that the Electric Sector, as a Critical Infrastructure support INL and the work they do. There is no substitute or other entity that is providing such quality service of such national importance."
4. Another utility security executive from American Electric Power recently testified to the value provided by INL through the DHS and DOE program: "The electricity industry is interested in continuing to work closely with DOE on the work being done at the Idaho National Laboratory. We believe it holds great promise as one of the best and most efficient means of stimulating research and developing technical solutions to the present shortfalls in cyber security." [Hearing Before the United States House of Representatives Science Committee, September 15, 2005].

Key Challenges in CIP and Cyber Security

As a result of operating and testing infrastructure systems, working with control system vendors and end users, INL is keenly aware of the key challenges in protecting critical control systems and the potential solutions to these complex challenges to ensure the security of our nation's critical infrastructure.

- **Increased Connectivity** – The use of open systems and more common technology combined with greater system access and available system knowledge has changed the risk profile of SCADA systems. These systems evolved in a less connected world relying on proprietary technologies which provided a sense of "security through obscurity" in the past. The control systems of today are more susceptible to security threats than before with SCADA vendors increasingly moving toward open industry standard protocols and platforms, system owners and operators providing greater access to market and accounting systems, regulatory requirements to share information and make systems available to all market participants and the greater use of public networks and wireless communications.
- **Interdependencies** – A further challenge arises from the reliance on telecommunication as an integral part of the overall control system. If SCADA and Energy Management Systems (EMS) are the brain stem and receptors of a control system, then Telecommunications represents the intricate network of nerve pathways that connects these operational assets, providing the means by which to deliver the control instructions and update system status. [The following provides a useful reference: Cyber Security: A Crisis of Prioritization, President's Information Technology Advisory Committee, February 2005]
- **Complexity** – A particular challenge is the complex and interconnected nature of critical control systems which can be found across many of the critical infrastructure sectors from directing advanced manufacturing systems to controlling the North American electric grid. If we focus on energy production and delivery, we find Process Control Systems (PCS) and specifically SCADA systems are used extensively throughout the electric, oil, and gas sectors to monitor and control processes that generate, transmit, transport and distribute energy.
- **Legacy Systems** – A significant portion of the control system technology in place today in many installations is old. These legacy systems were designed to operate over long lifecycles and were not designed with cyber security in mind. Hence, they are vulnerable to cyber attack and, in many cases, difficult to protect. In order to significantly lower the risk, we need to understand legacy system vulnerabilities and develop cost effective means to mitigate them without relying on new system deployments.
- **Deregulation** – Market forces, to include deregulation in the electric utility industry have increased the number of entities involved in the power life cycle from generation through transmission, distribution, metering, and billing; thus increasing reliance on and accuracy of information from third parties. Correspondingly, this has come with increased connectivity with outside vendors, customers, and business partners which have eroded the sanctity of the network perimeter. More connections through the perimeter inherently introduce more threats into the corporate networks.
- **System Accessibility** – The convergence of power company networks and the demand for remote access to these systems has rendered many SCADA systems accessible through non-SCADA networks. Specifically, connections between the grid and corporate networks for reporting purposes and outage management interfaces have the potential to expose the grid network to the threats experienced by the more common business network. [The following provides a useful reference: U.S.-Canada Power System Outage Task Force, August 14th Blackout: Causes and Recommendations, April 2004].

- **Offshore Reliance** – Cost pressures and technology support constraints have increased reliance on offshore development and system maintenance, thereby increasing the risk of intentional or unintentional security vulnerabilities. This risk is amplified as a result of ineffective/non-enforceable cyber laws in the respective offshore countries.
- **Information Sharing** – Finally, competitive pressure, legal liability risk and the lack of information protection mechanisms pose a significant barrier to information sharing between critical infrastructure stakeholders. This has significantly impeded the discovery and understanding of control system vulnerabilities, as well as the reporting of real-world incidents. [The following provides a useful reference: CRS Report for Congress – Government Activities to Protect the Electric Grid, October 2004].

  On the other hand, the knowledge revolution that has accompanied the Internet makes it easy to locate specific information regarding SCADA and automation systems. For example, "over 90% of major SCADA and Automation vendors have all of their manuals and specifications available online to the general public" (SCADA Security Strategy, PlantData). Easy access of such information to potential threat actors is a concern.

Recommendations

These challenges, although numerous and complex, are surmountable. There is an urgent need to accelerate the research, development, testing, and application of advanced control systems to enhance cyber security across the energy and other sectors. This need transcends individual companies, energy subsectors, and even the private sector. Toward this end, the Department of Homeland Security and the Department of Energy are supporting programs to facilitate and support risk reducing solutions. We, at INL, are focused on providing solutions to this key national need and have some recommendations for meeting the challenge.

SCADA/Cyber/Telecom Interconnect – We, as a nation, should develop an interdependent and inclusive view of control systems to include not only the SCADA systems but the cyber and Telecommunications functions that support them to ensure secure electrical power and industrial processes. SCADA, Cyber Security, and Telecommunications are areas where we must integrate research and testing efforts to understand how vulnerabilities impact the entire system. We at INL are already engaged with the telecommunication firms on interoperability and bandwidth issues, and we see the SCADA/Cyber/Telecom interconnectivity as the next area of pursuit.

The 21st Century could be characterized as a globally interconnected "flat world" (courtesy of Tom Friedman), which means hierarchical systems have to yield to horizontal and partnership-based enterprises. To that end, critical infrastructure protection, cyber security, and telecommunications particularly call to attention the interdependence between providers and markets so industries have a responsibility to work across sectors, and the same holds for the federal government. Furthermore, in the event of a manmade or natural disaster as in Katrina, active coordination across sectors is vital for timely response and expeditious recovery.

Minimum Standards – The electric sector, being at the hub of all, is active in securing its cyber and physical resources. Interim cyber security standards are in place in the electric sector, and they are moving through the approval process for a permanent, more expansive CIP standard. The final product should strengthen cyber security across the electric sector and lay the

groundwork for greater collaboration between industry and government. Similar efforts are underway through CIDX and much work remains to be done in all sectors of our infrastructure.

Develop Risk Assessment Tools – The federal government should continue to invest in the development of tools and provide required information to assist control systems security professionals to identify and address risk. Education and awareness efforts should be focused on developing an accurate understanding of risk to control systems. The NSTB Program and the CSSC program are both actively addressing this need and risk mitigation steps are beginning to be implemented at the user level.

Fixing Legacy Systems – Some type of incentive, either at the vendor level or user level, will go a long way to implement cyber security in legacy process control systems. Coupled with independent third party testing of the control system, through programs such as NSTB and CSSC, legacy systems could be upgraded with protective measures.

Information Protection – The electric infrastructure is one of the most critical infrastructures servicing the nation and maintaining our way of life. Certain technical, architectural and operational aspects and details must be kept secure so they will not be inadvertently disclosed to those who would try to disrupt or destroy our social, political or economic fabric. Yet there is a need to share the security aspects of the information with government and industry peers for benchmarking purposes while preserving competitive advantages. The same challenge applies to other sectors as well. This is an area where the use of trusted independent third party entities might prove beneficial and acceptable to all parties and merits further discussion.

Concluding Statement

Mr. Chairman and distinguished Members of the Committee, we at Idaho National Laboratory are fully committed to deliver on this important national mission, and along side DHS, DOE, and industry, we will strive to make our Laboratory the Center of Excellence in critical infrastructure protection to help end users. We welcome you to visit the Idaho National Lab to see firsthand the solutions we are providing to make our infrastructure safer. Again, I thank you for the opportunity to share these comments with you.